REMARKS

The specification was objected to as lacking section headings, and the Applicants are therefore tendering herewith a Substitute Specification in which only section headings have been added. No new matter has been added thereby.

Claims 41 and 42 were also objected to under 37 C.F.R. 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. Claims 41 and 42 have been cancelled and therefore this objection has been rendered moot. However, new claims that are being filed herewith that correspond to claims 41 and 42 do not contain multiple dependencies which depend from other multiple dependent claims.

Claims 27-40 have been rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention for the specific reasons set forth in numbered paragraph 6-14. Again, claims 27-40 have been cancelled, and new claims 53-68, which are based upon these canceled claims, have been rewritten to overcome all of the deficiencies noted by the Examiner that were present in claims 27-40.

Claims 27-40 have also been rejected under 35 U.S.C. §103(a) as being unpatentable over Rohatgi et al., U.S. Patent No. 5,625,693. For the reasons that follow, Applicants traverse the application of this reference to newly proposed claims 53-68.

The present application discloses a method for guaranteeing the integrity of data in a device, that does not perform the whole verification. The problem solved by the present invention is related to the reliability of the device containing the data.

According to the invention, the control center that transmitted the data takes part in the data checking in association with the security unit of the decoding unit. The data transmission implicates three items, namely, the control center that prepares the data, the decoder in which the data will be used, and the security unit that processes security operations.

An important aspect of the present invention is that the decoding unit does not have sufficient means to perform completely the integrity verification of the received data. The unit needs at least one other item for performing the verification, this item being considered as inviolable. Furthermore, according to this method, the awaited result of the verification is never transmitted to the decoding unit, so that a simulation of a correct verification is not possible.

The present invention is applied to decoding units.

The cited document US 5625693 (Rohatgi) describes a managing center that sends signed program modules or files to a receiver. The receiver determines in a stand-alone way the integrity of the provided data by comparing locally calculated hash values with the received ones. This document is not sufficient to enable a man skilled in the art to solve the problem of data integrity when the receiver is not secure enough. In fact, the complete verification is centralized in the receiver, and thus simulations of positive comparisons remains possible for a hacker. The verifying of the data integrity with a security unit independent of the receiver (decoder) and with the control center is not disclosed in the cited document. Therefore new independent claim 53 involves an inventive step over Rohatgi.

For these foregoing reasons, Applicants respectfully request entry of new claims 53-68, reconsideration of the present application in light thereof, and allowance of new claims 53-68 over all the prior art of record.

Respectfully submitted

By: _____

Clifford W. Browning
Reg. No. 32,201
Woodard, Emhardt et al. LLP
Bank One Center/Tower
111 Monument Circle, Suite 3700
Indianapolis, Indiana 46204-5137
(317) 634-3456

#341619